SCIENTIFIC REPORTS

OPEN

Enhancing structural robustness of scale-free networks by information disturbance

Received: 3 February 2017
Accepted: 5 July 2017
Published online: 08 August 2017

Jun Wu, Suo-Yi Tan, Zhong Liu, Yue-Jin Tan & Xin Lu

Many real-world systems can be described by scale-free networks with power-law degree distributions. Scale-free networks show a "robust yet fragile" feature due to their heterogeneous degree distributions. We propose to enhance the structural robustness of scale-free networks against intentional attacks by changing the displayed network structure information rather than modifying the network structure itself. We first introduce a simple mathematical model for attack information and investigate the impact of attack information on the structural robustness of scale-free networks. Both analytical and numerical results show that decreasing slightly the attack information perfection by information disturbance can dramatically enhance the structural robustness of scale-free networks. Then we propose an optimization model of disturbance strategies in which the cost constraint is considered. We analyze the optimal disturbance strategies and show an interesting but counterintuitive finding that disturbing "poor nodes" with low degrees preferentially is more effective than disturbing "rich nodes" with high degrees preferentially. We demonstrate the efficiency of our method by comparison with edge addition method and validate the feasibility of our method in two real-world critical infrastructure networks.

Networks are everywhere. Examples include the Internet, metabolic networks, electric power grids, supply chains, urban road networks, the world trade web, among many others. In the past few years, the discoveries of small-world[1] and scale-free[2] properties has stimulated a great deal of interest in studying the underlying organizing principles of various complex networks. The efforts to develop a universal view of complex networks have created both excitement and confusion about the way in which knowledge of network structure can be used to understand, control, or design system behavior[3]. The investigation of complex networks has become an important area of multidisciplinary area involving physics, mathematics, operations research, biology, social sciences, informatics, and other theoretical and applied sciences[4–9].

The functionality of complex networks relies on their structural robustness, i.e. the ability to retain its connectivity when a portion of their nodes or edges is removed[10, 11]. For example, modern society is dependent on its critical infrastructure networks: communication, electrical power, rail, and fuel distribution networks. Failure of any of these critical infrastructure networks can bring the ordinary activities of work and recreation to a standstill[12–14]. Terrorist attacks on transportation networks have traumatized modern societies. With a single blast, it has become possible to paralyze airline traffic, electric power supply, ground transportation or Internet communication. Other examples of structural robustness arise in nature, such as the robustness of food webs to biodiversity loss[15, 16].

Because of its broad applications, the structural robustness of complex networks has received increasing attention, especially from the original work by Albert *et al.*[17]. They introduced two attack strategies, i.e., random failure and intentional attack. Albert *et al.* suggested that scale-free networks characterized by a highly heterogeneous degree distribution are robust against random failure but are very fragile against intentional attack. This property is referred to as the "robust yet fragile" feature or the Achilles' heel of scale-free networks by Doyle *et al.*[18, 19]. Because of the ubiquity of scale-free networks in natural and man-made systems, the structural robustness of scale-free networks has been of great interest since the discovery of the scale-free property.

Let's recall the "robust yet fragile" feature of scale-free networks. From the perspective of attack information, random failure and intentional attack are merely two extremes in real-world networks. With the perfect attack

College of Information System and Management, National University of Defense Technology, Changsha, Hunan, 410073, P. R. China. Correspondence and requests for materials should be addressed to J.W. (email: junwu@nudt.edu.cn) or Z.L. (email: philipliu@263.com)

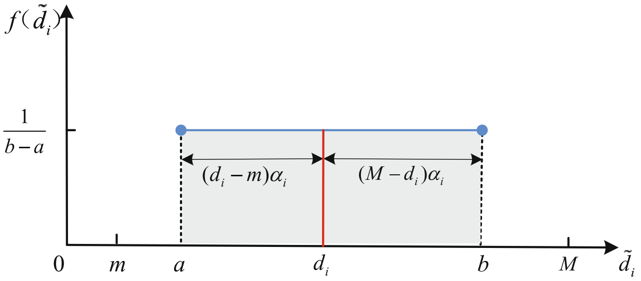

Figure 1. Illustration of the mathematical model of attack information. $f(\tilde{d}_i)$ is the probability density function of the displayed degree $\tilde{d}_i$. The information perfection parameter α_i characterizes the variability of the displayed degree $\tilde{d}_i$.

information, one can remove the most important nodes preferentially according to some attack criteria, of which the most common is the degree of nodes. This attack strategy corresponds to the intentional attack. Without any attack information, one can only remove the nodes randomly. This attack strategy corresponds to the random failure. Information as an existence or expression format of thing's movement is a common property of all matters. The robust-yet-fragile feature of scale-free networks reveals that the attack information can make an enormous difference of structural robustness. It inspires us to consider enhancing the structural robustness against intentional attacks by changing the displayed network structure information rather than modifying the network structure itself. If we can reduce the perfection of attack information by information disturbance, the critical hub nodes may survive during the intentional attacks and then the structural robustness of scale-free networks will be remarkably enhanced. To the best of our knowledge, this idea is new.

Results

Measuring the perfection of attack information.

Consider networks formalized in terms of a simple undirected graph $G(V, E)$, where V is the set of nodes and E is the set of edges. Denote by $N = |V|$ the number of nodes. Denote by k_i the degree of node v_i and denote by $p_d(k)$ the degree distribution. If the degree distribution follows a power law, i.e., $p_d(k) = ck^{-\lambda}(m \le k \le M)$, where m is the minimum degree and M is the maximum degree of G, a network is called a scale-free network with the scaling exponent λ. The power-law distribution implies that nodes with only a few edges are numerous, but a very few nodes have a large number of edges. Due to the ubiquity of scale-free networks in the real-world, we focus on the structural robustness of scale-free networks in this study.

We only consider the node attack approaches in this study and assume that the attached edges are removed if one node is removed. We employ the degree of each node as the attack criterion, which means that the attacker will remove nodes in decreasing order of the degrees of nodes. We remark that the attack criterion has no essential effect on our model. Noting that the attacker may not obtain the perfect information, we denote by $\tilde{d}_i$ the displayed degree of a node v_i from the view of attacker and define it as the attack information. Although the true degree of a node is the objective existence, the displayed degree d_i will be generally different from the true degree d_i. To measure the deviation from the displayed degree to the true degree, the displayed degree $\tilde{d}_i$ is supposed to spread out from the true degree towards the minimum node degree m and the maximum node degree M proportionately. For the purpose of convenience, we assume that the displayed degree $\tilde{d}_i$ follows a uniform distribution $U(a, b)$ as shown in Fig. 1, where the minimum value

$$a = d_i - (d_i - m)(1 - \alpha_i) = d_i\alpha_i + m(1 - \alpha_i) \tag{1}$$

and the maximum value

$$b = d_i + (M - d_i)(1 - \alpha_i) = d_i\alpha_i + M(1 - \alpha_i). \tag{2}$$

Here, the perfection parameter of attack information $\alpha_i \in [0, 1]$ characterizes the variability of the displayed degree $\tilde{d}_i$. The larger α_i is, the narrower the distribution region is and then the more perfect the attack information is. There are two extreme cases. If $\alpha_i = 0$ for all nodes, $\tilde{d}_i$ follows a uniform distribution in the region $[m, M]$, which corresponds to the random failure. If $\alpha_i = 1$ for all nodes, we obtain $\tilde{d}_i = d_i$, which corresponds to the intentional attack.

It is easy to obtain that the expectation of the displayed degree of a node v_i is

$$E(\tilde{d}_i) = \frac{a + b}{2} = d_i\alpha_i + \frac{(m + M)(1 - \alpha_i)}{2} \tag{3}$$

and the standard deviation is

$$\sigma(\tilde{d}_i) = \frac{(b - a)}{2\sqrt{3}} = \frac{(m + M)(1 - \alpha_i)}{2\sqrt{3}}. \tag{4}$$

We remark that the fluctuation interval of the displayed degree $\tilde{d}_i$ of a node v_i may not be symmetrical around its true degree d_i. If $d_i < (m + M)/2$, then $E(\tilde{d}_i) = d_i\alpha_i + (m + M)(1 - \alpha_i)/2 > d_i$; if $d_i > (m + M)/2$, then

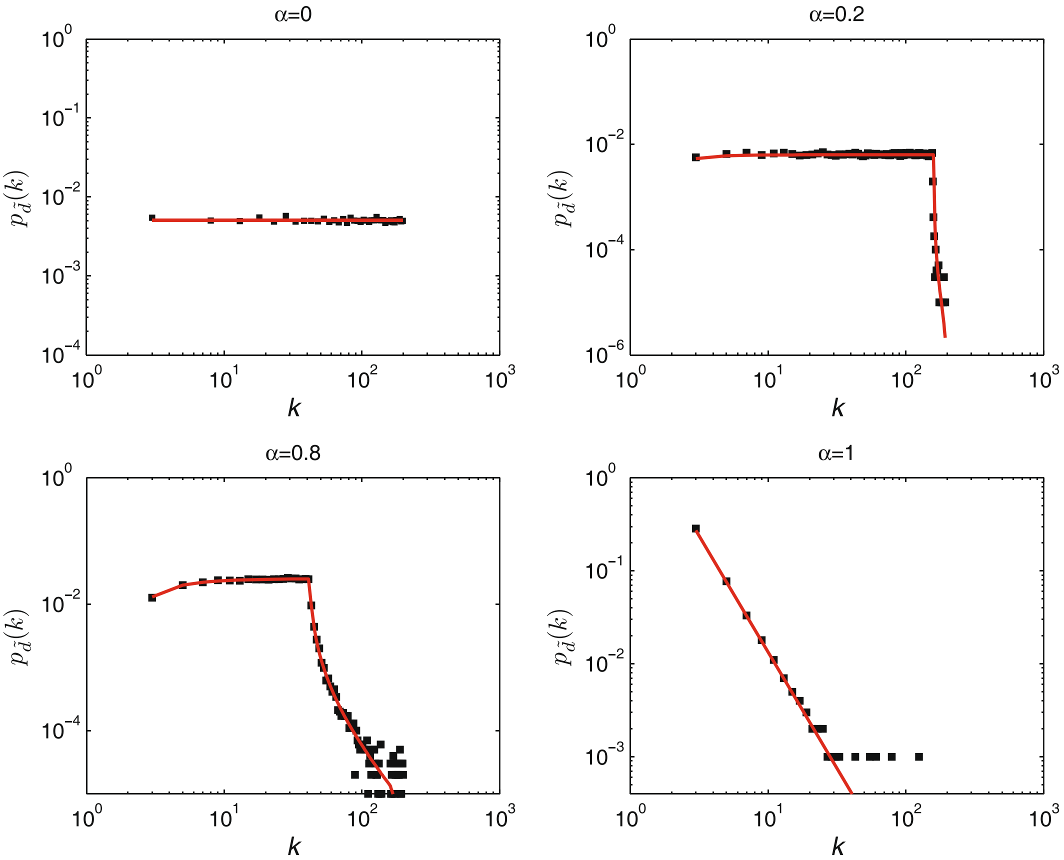

Figure 2. The displayed degree distribution (in a log-log scale) for various attack information perfection parameter α in a random scale-free network. The degree distribution follows $p_d(k) = (\lambda - 1)m^{\lambda-1}k^{-\lambda}$, where $N = 1000$, $\lambda = 2.5$ and $m = 2$. The simulation results are averaged over 100 independent realizations of imperfect attack information. The solid lines correspond to the analytical results (see Methods).

$E(\tilde{d}_i) = d_i\alpha_i + (m + M)(1 - \alpha_i)2 < d_i$. It suggests that the deviation from the displayed degree to the true degree may come from both the inaccuracy and the imprecision of attack information, where the accuracy refers to the closeness of agreement between a measurement and the true value, and the precision refers to the closeness of agreement of a set of measurements.

Impact of attack information on structural robustness. To explore the impact of attack information, we first show in Fig. 2 the displayed degree distribution $p_{\tilde{d}}(k)$ in random scale-free networks[20], which is determined by the degree distribution $p_d(k)$ and the attack information perfection α_i. For the purpose of convenience, let's suppose that the attack information perfection α_i for all nodes is identical, i.e., $\alpha_i = \alpha$, $i = 1, 2, \ldots, N$. We find that the displayed degree distributions gradually deviate from power-law distributions as the attack information perfection parameter α decreases.

We show the relative sizes of the largest component S as the removal fraction of nodes f increases for various attack information perfection parameter α in Fig. 3. It is easy to see that the attack information perfection has a considerable impact on S. If the attack information perfection parameter α is small, for example $\alpha = 0.2$, the relative size of the largest component decreases slowly with the increasing of removal fraction of nodes and survives until a large fraction of the nodes are removed. However, if the attack information perfection parameter α is large, the S decreases abruptly at a small critical value of f.

Figure 4(a) shows the critical removal fraction f_c as a measure of network robustness[17] both from the numerical and analytical results (see Methods). We observe that increasing the attack information perfection remarkably reduces the structural robustness of scale-free networks. From another perspective, we can enhance the structural robustness of scale-free networks by decreasing the perfection of attack information. For example, when $m = 2$, if we can decrease the attack information perfection parameter by information disturbance from $\alpha = 1$ to $\alpha = 0.8$, the critical removal fraction f_c can be increased from 23% to 63%. This means that information disturbance is an efficient strategy to enhance the structural robustness of scale-free networks. Moreover, we report the network robustness measure R[21, 22] as a function of the attack information perfection parameter α in Fig. 4(b) and observe the similar results as the case of f_c. When $m = 4$, if we can decrease the attack information perfection by information disturbance from $\alpha = 1$ to $\alpha = 0.8$, the network robustness measure R can be increased from 0.3041 to 0.3834.

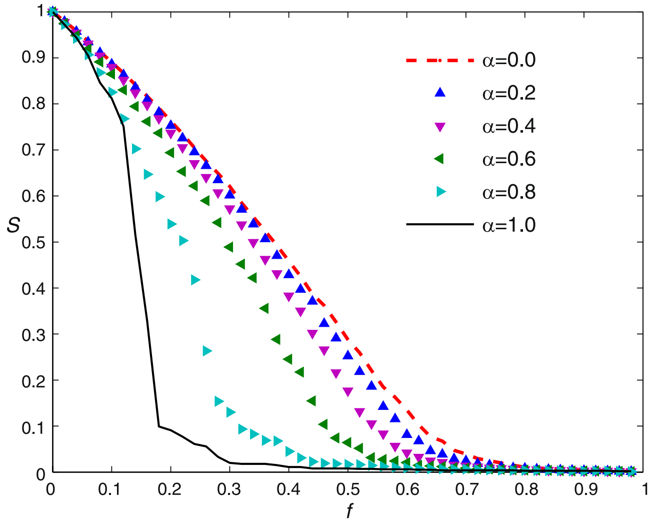

Figure 3. The relative sizes of the largest component S versus f for various attack information perfection parameter α. The original network is the same as the one we used in Fig. 2. The simulation results are averaged over 100 independent realizations of imperfect attack information.

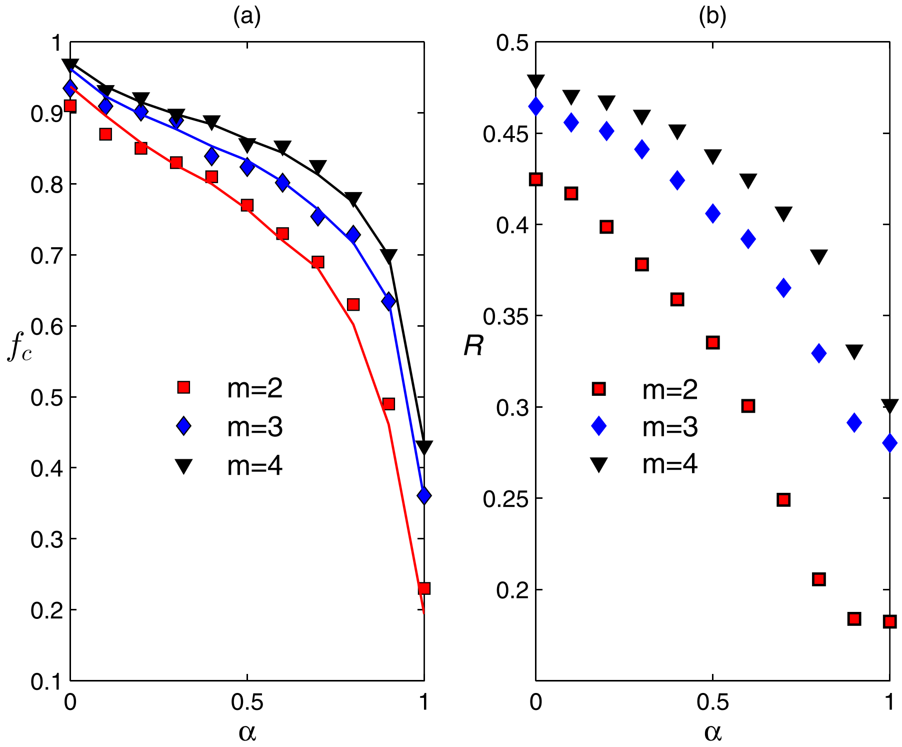

Figure 4. The critical removal fraction of nodes f_c (**a**) and network robustness R (**b**) versus attack information perfection parameter α in random scale-free networks. The degree distributions follow $p_d(k) = (\lambda - 1)m^{\lambda-1}k^{-\lambda}$, where $N = 1000$, $\lambda = 2.5$, $m = 2$ (■), $m = 3$ (◆) and $m = 4$ (▼). The simulation results are averaged over 100 independent realizations of imperfect attack information. The solid lines correspond to the analytical results.

Optimization model for disturbance strategies with cost constraint. In most realistic cases, we can not simultaneously disturbance all the nodes due to the cost constraint. Denote by $\beta_i = 1 - \alpha_i \in [0, 1]$ the disturbance strength parameter of a node v_i, which represents the magnitude of information disturbance for the node v_i. We call the vector $B = [\beta_1 \beta_2 \ldots \beta_N]$ a disturbance strategy. We define a categorical variable η_i for each node v_i that $\eta_i = 1$ if the node v_i is disturbed, otherwise $\eta_i = 0$, i.e.,

$$\eta_i = \begin{cases} 1 & \text{if } \beta_i > 0 \\ 0 & \text{if } \beta_i = 0 \end{cases}. \tag{5}$$

We denote by $\omega = \frac{1}{N}\sum_{i=1}^{N} \eta_i$ the disturbance range parameter. The case of $\omega = 1$ has been studied in the previous section.

According to our mathematical model for attack information, the displayed degree of a node after information disturbance is a random variable rather than a definite value before information disturbance. We suppose that the uncertainty of the displayed degree of a node determines the of disturbance cost for it. The more uncertain the displayed degree of a node is, the costlier the disturbance strategy. We use the standard deviation of displayed degree of a node given in Eq. (4) to characterize the uncertainty of the displayed degree of a node and define the disturbance cost of a disturbance strategy as the sum of standard deviation of displayed degree for all nodes

$$C = \sum_{i=1}^{N} \sigma(\tilde{d}_i) = \sum_{i=1}^{N} \frac{(m + M)(1 - \alpha_i)}{2\sqrt{3}} = \frac{\sqrt{3}(m + M)}{6}\sum_{i=1}^{N} \beta_i. \tag{6}$$

Because $0 \le \beta_i \le 1$, it is easy to obtain that the maximum disturbance cost is $C_{max} = \sqrt{3}(m + M)N/6$ corresponding to the complete disturbance strategy $B_{max} = [11\ldots1]$. In most cases, the disturbance cost is limited. We define the cost constraint as follows

$$\hat{C} = C_{max} \cdot \theta = \frac{\sqrt{3}(m + M)N}{6}\theta, \tag{7}$$

where $\theta \in [0, 1]$ is the cost constraint parameter. The larger the cost constraint parameter θ is, the more loose the constraint of disturbance cost is; the smaller the cost constraint parameter θ is, the tighter the constraint of disturbance cost is. In the extreme case of $\theta = 0$, no nodes can be disturbed; in the extreme case of $\theta = 1$, all nodes can be completely disturbed. The cost constraint condition $C \le \hat{C}$ leads to

$$\sum_{i=1}^{N} \beta_i \le N \cdot \theta. \tag{8}$$

Our goal is to enhance the structural robustness by choosing the disturbance strategy $B = [\beta_1\ \beta_2\ldots\beta_N]$ given the cost constraint parameter θ. Thus we define the effect of a disturbance strategy as

$$\Phi(B) = |\Gamma(B)|, \tag{9}$$

where Γ is the structural robustness measure, such as f_c or R (see Methods), and $|\Gamma(B)|$ represents the expectation of the structural robustness measure under a disturbance strategy B. Thus, the optimization model of disturbance strategies can be described as follows

$$\begin{aligned} &\max\ \Phi(B = [\beta_1\beta_2\ldots\beta_N]) \\ &\text{s.t.} \begin{cases} \sum_{i=1}^{N} \beta_i \le N \cdot \theta \\ 0 \le \beta_i \le 1 \end{cases}. \end{aligned} \tag{10}$$

For large N, it will be a large-scale optimization problem[23], which is very time-consuming. For the convenience of analysis, we next consider a simplified version of the optimization model presented above. We assume that the disturbance strength parameters β_i for all the disturbed nodes ($\eta_i = 1$) are identical, i.e.,

$$\beta_i = \beta \cdot \eta_i. \tag{11}$$

where $\beta \in (0, 1]$. Thus the disturbance cost can be written as

$$C = \frac{\sqrt{3}(m + M)}{6}\sum_{i=1}^{N} \beta_i = \frac{\sqrt{3}(m + M)\beta}{6}\sum_{i=1}^{N} \eta_i, \tag{12}$$

and then the optimization model for disturbance strategies can be transformed into

$$\begin{aligned} &\max\ \Phi(B = \beta \cdot [\eta_1\eta_2\cdots\eta_N]) \\ &\text{s.t.} \begin{cases} \beta \cdot \sum_{i=1}^{N} \eta_i \le N \cdot \theta \\ \eta_i = 0, 1 \\ 0 < \beta \le 1 \end{cases}. \end{aligned} \tag{13}$$

It means that the optimization problem is just simplified to determine the node set to disturb and the magnitude of information disturbance.

According to the analysis above, we know that the disturbance effect Φ decreases monotonically as the attack information perfection parameter α increases and hence increases monotonically as the disturbance strength parameter β increases. Therefore, to maximize Φ, the parameter β should take the maximum value under the conditions of constraint $\beta \cdot \sum_{i=1}^{N} \eta_i \leq N \cdot \theta$ and $0 < \beta \leq 1$, which leads to

$$\beta = \begin{cases} N \cdot \theta / \sum\limits_{i=1}^{N} \eta_i & \text{if} \sum\limits_{i=1}^{N} \eta_i > N \cdot \theta \\ 1 & \text{if} \sum\limits_{i=1}^{N} \eta_i \leq N \cdot \theta \end{cases}. \tag{14}$$

Noting that $\sum_{i=1}^{N} \eta_i = N \cdot \omega$, then we obtain that

$$\beta = \begin{cases} \theta/\omega & \text{if } \omega > \theta \\ 1 & \text{if } \omega \leq \theta \end{cases} \text{ or } \beta = \min\{\theta/\omega,\ 1\}. \tag{15}$$

Thus the optimization model for disturbance strategies presented in Eq. (13) can be written as

$$\begin{aligned} &\max \Phi(B = \min\{\theta/\omega, 1\} \cdot [\eta_1 \eta_2 \cdots \eta_N]) \\ &\text{s.t. } \eta_i = 0, 1 \end{aligned} \tag{16}$$

It means that the optimization problem is just simplified to determine how many and which nodes should be disturbed.

To determine which nodes are disturbed, we transform the process of determining into an unequal probability sampling problem without replacement. We define the selection probability that a node v_i is sampled to disturb in each sample as follows

$$\nabla_i = \frac{d_i^{\delta}}{\sum_{t=1}^{N} d_t^{\delta}}, \tag{17}$$

where $\delta \in [-1, 1]$ is the disturbance strategic parameter. If $\delta > 0$, the high-degree nodes are disturbed preferentially; if $\delta < 0$, the low-degree nodes are disturbed preferentially; if $\delta = 0$, the nodes are disturbed randomly. Consequently, the simplified version of optimization model for disturbance strategies can be described as follows

$$\begin{aligned} &\max \Phi(B = \Theta(\omega, \delta)) \\ &\text{s.t. } \begin{cases} 0 \leq \omega \leq 1 \\ -1 \leq \delta \leq 1 \end{cases}, \end{aligned} \tag{18}$$

where $\Theta:(\omega, \delta) \rightarrow B$ corresponds to the procedure of unequal probability sampling.

Optimal disturbance strategies for enhancing structural robustness. We next investigate the optimal disturbance strategies for enhancing structural robustness based on the simplified optimization model in Eq. (18). Because the calculation of structural robustness measure Γ might be computationally expensive, and furthermore, we need to take the average over many realizations of disturbance strategy to evaluate the disturbance effect Φ, the exploration of the solution space are largely limited. Therefore, we consider to use the statistical approximations to construct a meta-model, which provides a surrogate model of the original optimization problem. The surrogate model can be estimated from experiment data by running the simulation experiments on a sample of points in the region of interest. We employ the popular Kriging surrogate models[24] in this study. We show the Kriging-based response surface and contour plots for the disturbance effect in Fig. 5.

From the response surface and the contour plots in Fig. 5, we surprisingly find that the disturbance effect decreases monotonically with the increase of disturbance strategic parameter δ given the disturbance range parameter ω. We observe similar results in scale-free networks with various parameters. It suggests that, given the disturbance range parameter ω, disturbing the "poor nodes" with low degrees may be more effective in scale-free networks, i.e., the optimal disturbance strategic parameter is $\delta^* = -1$. This observation is counterintuitive but interesting. To explain this phenomenon, we sort all nodes in decreasing order of their degrees d_i before information disturbance and their displayed degrees $\tilde{d}_i$ after information disturbance, respectively. Denote by r_i and $\tilde{r}_i$ the rank of v_i before and after information disturbance, respectively. In Fig. 6, we plot the degree pairs $(d_i, \tilde{d}_i)$ and the rank pairs $(r_i, \tilde{r}_i)$ under three typical disturbance strategies: (1) "rich nodes strategy" with $\delta = 1$; (2) "random nodes strategy" with $\delta = 0$; (3) "poor nodes strategy" with $\delta = -1$. Under the "rich nodes strategy", we observe that the degrees of high-degree nodes change a lot after information disturbance, but their ranks change very little and then the small "rich group" remains basically unchanged. It leads to the fact that high-degree nodes will still be removed after information disturbance. However, under the "poor nodes strategy", we observe that both the degrees and the ranks of low-degree nodes change a lot after information disturbance and then many "poor nodes" infiltrate the "rich group" after information disturbance. Thus, the high-degree nodes can survive during the attack. These findings suggest that what really matters to the enhancement of structural robustness is the change of ranks of nodes rather than the change of the degrees of nodes itself. Due to the heterogeneous degree distributions, the "poor nodes strategy" disturbs the ranks of nodes in scale-free networks more dramatically and then is more effective than the "rich nodes strategy".

To verify this judgment, we implement similar experiments in Erdös-Rényi (ER) random graphs[25] and show the results in Fig. 7. The ER random graph $G_{N,p}$ is obtained by starting with a set of N nodes and adding edges

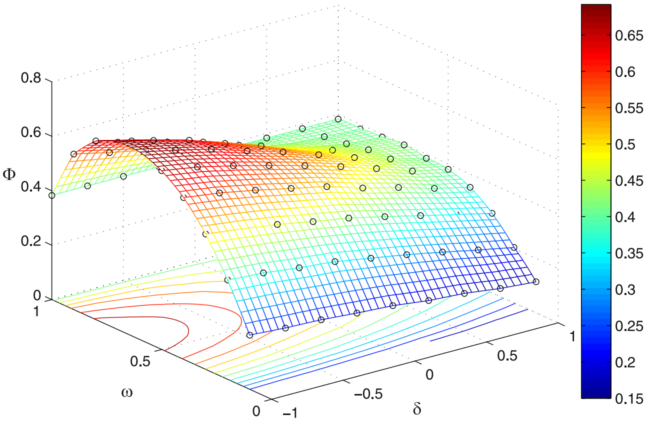

Figure 5. The Kriging-based response surface and contour plots for the disturbance effect. The original network is the same as the one we used in Fig. 2. The cost constraint parameter θ is 0.1. The circles represent the original experiment data, which are averaged over 100 realizations of disturbance strategy. The disturbance effect is obtained based on the structural robustness measure R.

between them at random such that each of the possible $N(N-1)/2$ edges occurs independently with probability p. The ER random graph has a Poisson degree distributions for large N such that most nodes in the network have similar degrees. In contrast to the case of scale-free networks, we find that the "rich nodes strategy" seems to be more effective than the "poor nodes strategy" in ER random graphs. This result can also be explained by our observation that many high-degree nodes can survive after information disturbance under the "rich nodes strategy", while the "rich group" remains almost unchanged under the "poor nodes strategy".

We next investigate the optimal disturbance range parameter ω for enhancing structural robustness of scale-free networks. We show in Fig. 8 the relationship between the disturbance effect Φ and the disturbance range parameter ω under the "poor nodes strategy" ($\delta^*=-1$). We observe that the disturbance effect Φ achieves a maximum value Φ^* (see the inset in Fig. 8) at the optimal disturbance range parameter ω^*. We find that, even with a very small cost constraint parameter $\theta=0.05$, the maximum disturbance effect Φ^* can be increased from 0.1433 (intentional attack without information disturbance) to 0.2897. In other words, disturbance with an average disturbance strength parameter 0.05 can almost double the structural robustness of scale-free networks. Moreover, we observe that, if the cost constraint parameter θ increases to 0.5, the maximum disturbance effect Φ^* can achieve to the case of random failure (0.4361).

We show in Fig. 9 the optimal disturbance range parameter ω^* and the corresponding optimal disturbance strength parameter β^* based on Eq. (15) as a function of the cost constraint parameter θ. We can obtain the optimal disturbance strategies with various cost constraint parameters θ. For example, with $\theta=0.05$, we should disturb about 50% nodes with the disturbance strength parameter 0.1. We find that the optimal disturbance range parameter ω^* firstly increase rapidly as the cost constraint parameter θ increases and then achieve to a stable value when θ is large. Moreover, we find that the optimal disturbance strength parameter β^* increase approximately linearly as the cost constraint parameter θ increases.

Comparison with other approach for enhancing structural robustness. To furthermore demonstrate the efficiency of our method, we next compare our method with the edge addition method. In each step of the edge addition method, we add randomly one nonexistent edge to enhance the structural robustness. We show in Fig. 10 the number of edges needed to be added to achieve the same structural robustness measure with various cost constraint parameters θ. We find that we need to add near 600 edges to achieve the same effect even with the small cost constraint parameter $\theta=0.05$. It indicates that enhancing structural robustness of scale-free networks against intentional attacks by information disturbance is a cost-efficient approach.

Experiments in real-world networks. Modern society is dependent on well-functioning infrastructure. To valid the feasibility of our method, we consider two of the most fragile, but critical infrastructures: the power grid and the fiber network. The breakdown of any of these networks would constitute a major disaster due to the strong dependency of modern society on energy and information. We here apply our method to the India power grid[26] consisting of $N=572$ nodes and $W=871$ edges and the fiber backbone operated by a major U.S. network provider (CenturyLink) consisting of $N=154$ nodes and $W=206$ edges. Both networks have power-law degree distributions.

We first calculate the original structural robustness measure R^0 for the India power grid (IPG) and the U.S. fiber network (USF). It is obtained that $R_{IPG}^0=0.0912$ and $R_{USF}^0=0.1341$. We then use the method introduced above to explore the optimal disturbance strategies with various cost-constrain parameters. The results are shown in Table 1. It is easy to find that the structural robustness of both IPG and USF is dramatically enhanced by the information disturbance. For example, with the cost constraint parameter $\theta=0.3$, the optimal disturbance strategy can almost double the structural robustness of IPG from $R_{IPG}^0=0.09$ to $\Phi^*=0.1801$. Moreover, we see that, for both IPG and USF, the optimal disturbance strategy is try to disturb intensively the "poor nodes" with low degrees ($\delta^*=-1$) with high disturbance strength parameter ($\beta^*\approx 1$).

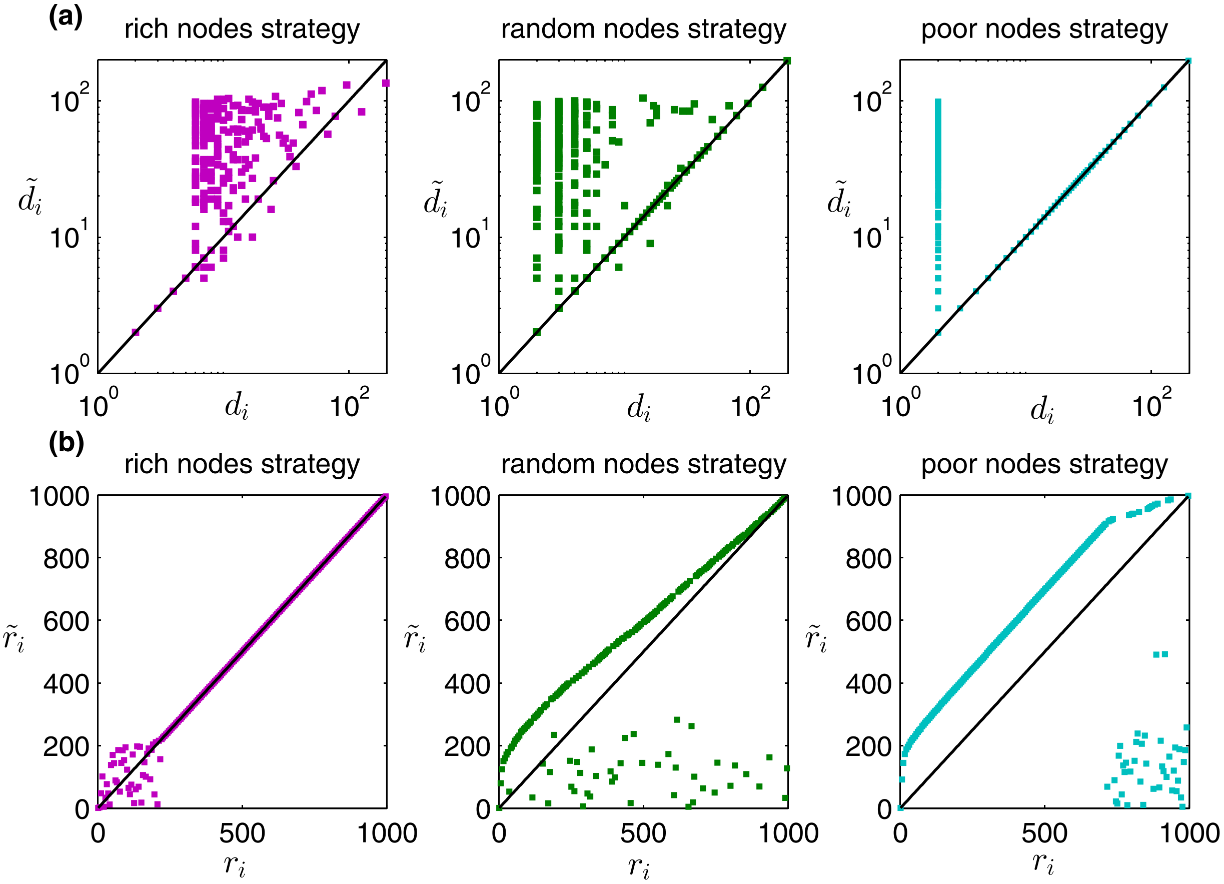

Figure 6. Degree pairs (**a**) and rank pairs (**b**) of nodes before and after information disturbance under three typical disturbance strategies. The original network is the same as the one we used in Fig. 2. The cost constraint parameter θ is 0.1 and the disturbance range parameter ω is 20%. The solid lines are the reference lines which represent that $d_i = \tilde{d}_i$ or $r_i = \tilde{r}_i$.

Discussions

Many real-world systems can be described by scale-free networks with power-law degree distributions, leading to the "robust yet fragile" feature. The enhancement of structural robustness of scale-free networks against intentional attack is an important and challenging problem. In this study, we assumed that the attacker removes nodes according to some attack criteria, of which the most common is the degree of nodes. Then the attack criterion can be considered as the attack information. With perfect attack information, one can preferentially remove the most important nodes in the network (intentional attack). However, in many realistic settings, the attacker can not obtain perfect attack information. For example, the displayed degree of nodes from the view of the attacker may deviate from the true degree. Thus, the attacker wants to gain the attack information as much as possible to destroy a network using various reconnaissance means, whereas the defenders want to conceal the attack information as much as possible to protect a network using various disturbance means. It inspires us to consider enhancing the structural robustness against intentional attacks by changing the displayed network structure information rather than modifying the network structure itself.

We first introduced a mathematical model for attack information based on the node degree. Instead of a certain value, we assumed that the displayed degree $\tilde{d}_i$ with imperfect attack information is a random variable following a uniform distribution, which can be controlled by a normalized perfection parameter $\alpha_i \in [0,1]$. With this assumption, we can derive analytically the displayed degree distribution and the measure of structural robustness with the imperfect attack information. It is worth mentioning that, even we use degree in the model, the method can be readily extended to other attack criteria, such as node betweenness, closeness, etc. We investigated the impact of attack information on the structural robustness of scale-free networks both analytically and numerically. It was shown that reducing the attack information perfection by information disturbance can dramatically enhance the structural robustness of scale-free networks. We then proposed a generalized and simplified optimization model of disturbance strategies. In the simplified optimization model, it is assumed that the disturbance strength parameter for all the disturbed nodes is identical. We solved the simplified optimization model based on the Kriging-based response surface. Intuitively, one should disturb "rich nodes" with high degrees preferentially to enhance the structural robustness. But we found with surprise that, with cost constraints, disturbing "poor nodes" with low degrees is more effective in scale-free networks. We explained this counterintuitive phenomenon by comparing with Erdös-Rényi (ER) random graphs and emphasized that it stems from the heterogeneous

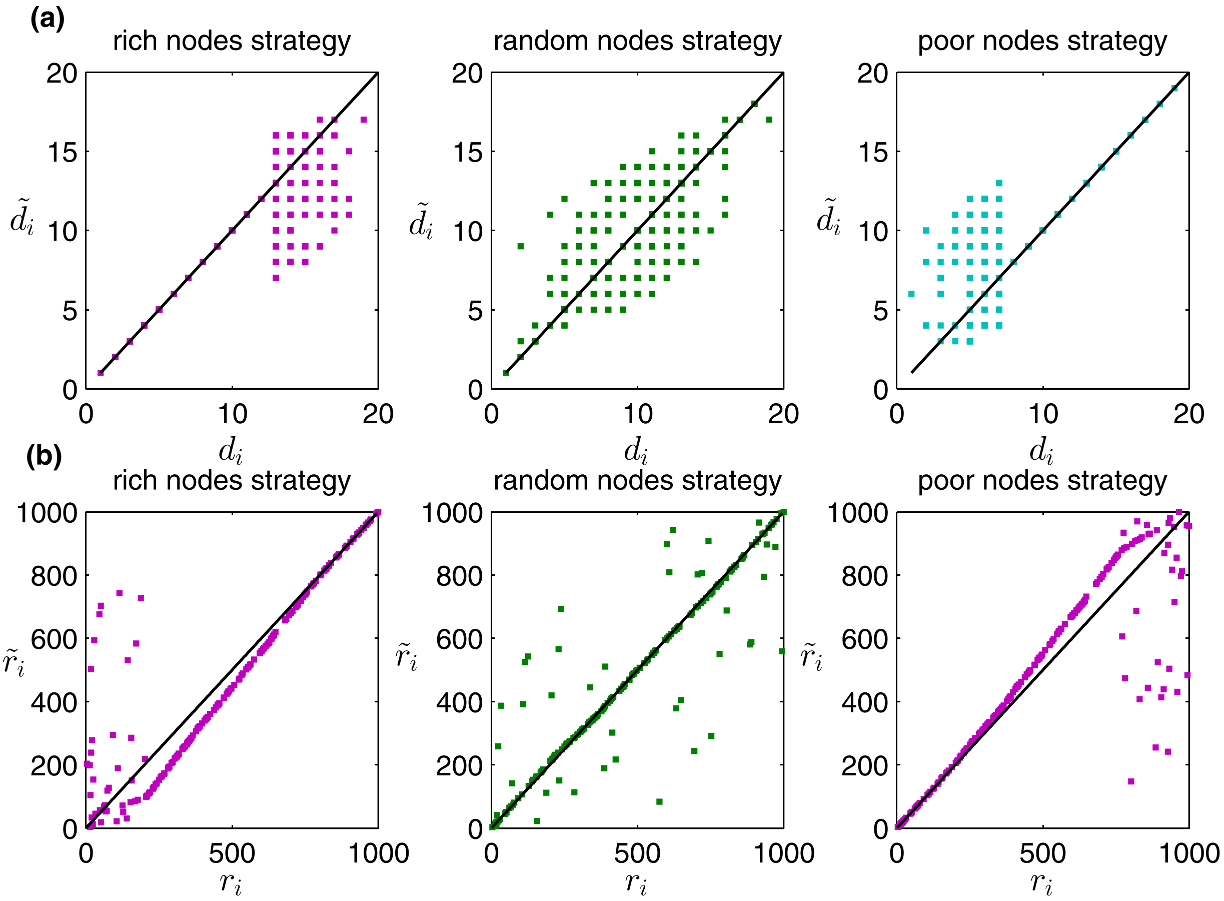

Figure 7. Degrees (**a**) and ranks (**b**) of nodes before and after information disturbance under three typical disturbance strategies. The original network is an ER random graph $G_{N,p}$, where $N = 1000$ and $q = 0.01$. The cost constraint parameter θ is 0.1 and the disturbance range parameter ω is 20%. The solid lines are the reference lines which represent that $d_i = \tilde{d}_i$ or $r_i = \tilde{r}_i$.

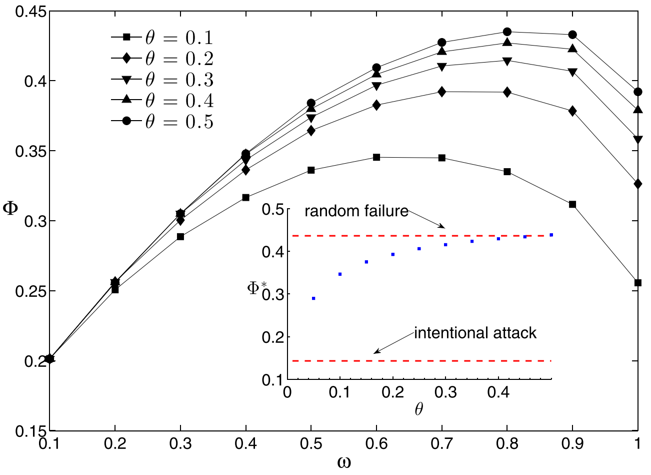

Figure 8. The disturbance effect Φ versus the disturbance range parameter ω under the "poor nodes strategy". The original network is the same as the one we used in Fig. 2. The symbols represent the original experiment data, which are averaged over 100 realizations of disturbance strategy. The solid lines are obtained from the Kriging surrogate model. The insert shows the maximum disturbance effect Φ^* as a function of the cost constraint parameter θ and the cases of random failure and intentional attack as references (dotted lines). The disturbance effect is obtained based on the structural robustness measure R.

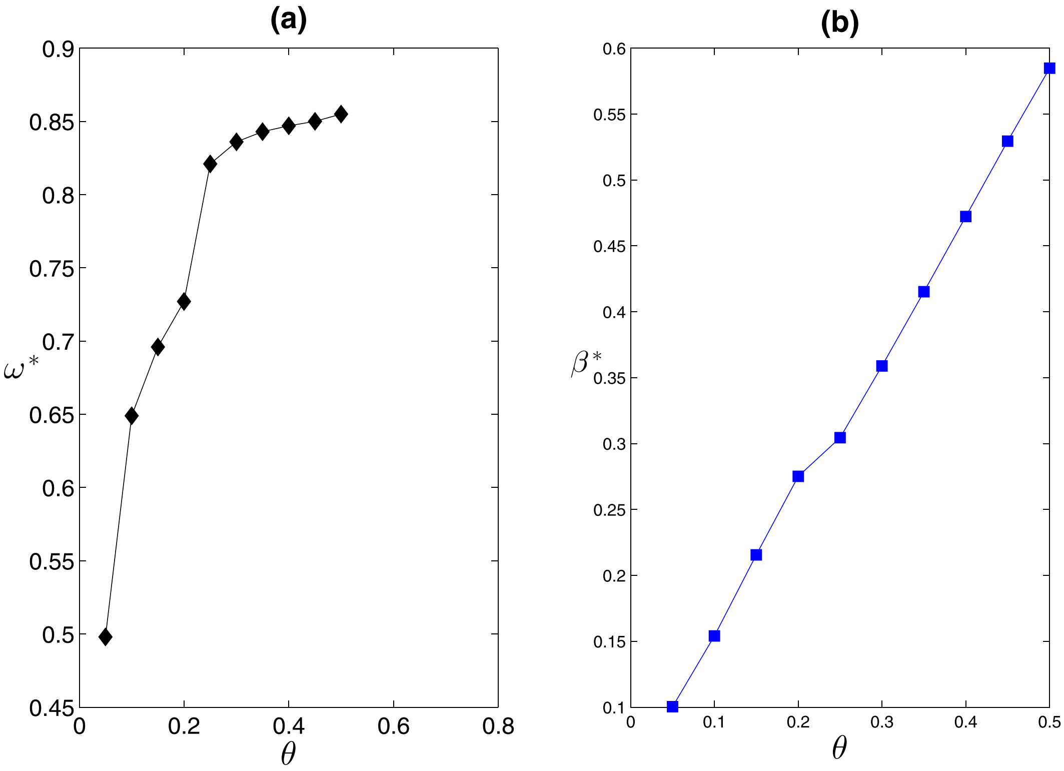

Figure 9. The optimal disturbance range parameter ω^* (**a**) and the optimal disturbance strength parameter β^* (**b**) versus the cost constraint parameter θ. The original network is the same as the one we used in Fig. 2. The disturbance effect is obtained based on the structural robustness measure *R*.

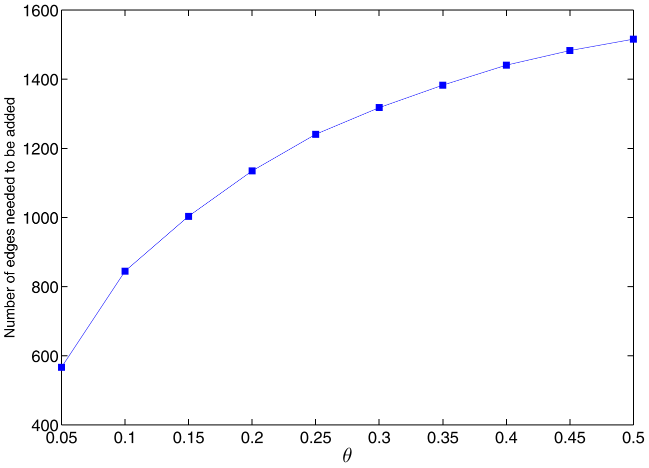

Figure 10. The edge addition method versus the information disturbance method. The original network is the same as the one we used in Fig. 2. The disturbance effect is obtained based on the structural robustness measure *R*.

	$\theta = 0.1$				$\theta = 0.2$				$\theta = 0.3$			
Networks	δ^*	ω^*	β^*	Φ^*	δ^*	ω^*	β^*	Φ^*	δ^*	ω^*	β^*	Φ^*
IPG	−1	0.10	1	0.1245	−1	0.20	1	0.1548	−1	0.30	1	0.1801
USF	−1	0.11	0.9091	0.1605	−1	0.20	1	0.1799	−1	0.31	0.9677	0.1976

Table 1. The optimal disturbance strategies in two real-world critical infrastructure networks. IPG represents the India power grid and USF represents the U.S. fiber network.

degree distributions of scale-free networks. It is worth noting that this finding is based on the assumption of identical disturbance strength parameters. The optimal disturbance strategy with non-identical disturbance strength parameters remains an open and challenging problem. Lastly, we demonstrated the efficiency of our method by comparing with the edge addition method and validate the feasibility of our method in two real-world critical infrastructure networks, i.e., the India power grid and the U.S. fiber network. Although our results can not apply to all networks with various degree distributions, it is of great significance because of the ubiquity of scale-free networks.

It is intuitive to enhance structural robustness of scale-free networks against intentional attacks by information disturbance. The fundamental objective of this approach is to make important nodes less distinguishable with less important nodes by information disturbance, and thus the important nodes can survive during the intentional attacks. In most cases, changing the displayed information of network structure is easier and more realistic than reconstructing the network. Although we didn't give the practical disturbance scheme from a technical perspective, the main contribution of this paper is to present a general theoretical framework and demonstrate the efficiency and the feasibility of this method from a methodological perspective. We believe that our model and findings may lead to useful insights on developing effective attack or defense strategies in scale-free networks, so as to protect infrastructure systems (e.g., power grids, telecommunications, transportation and water-supply systems) against terrorist attacks, or reduce undesired highly synchronized behavior in the central nervous system (e.g., Parkinson's disease, epilepsy, and other pathological rhythmic activities), etc.

Methods

Measures of structural robustness with imperfect attack information. Simple and effective measures of structural robustness are essential for the study of network resistance. We first consider the critical removal fraction of nodes to characterize the structural robustness of scale-free networks with imperfect attack information[17, 27]. It characterizes statistically how the removal of nodes leads to the disintegration of the network at a given critical removal fraction f_c. The larger the f_c is, the more robust the network is. The disintegration of a network is measured in terms of network performance, which is characterized most often with the size of the largest component. In this study, we choose $\kappa \equiv <k^2>/<k> <2$ as the criterion for determing the disintegration of a network[28, 29]. After each node is removed, we calculate κ. When κ becomes less than 2, we record the number of nodes t removed up to that point. The threshold f_c is obtained as $f_c = <t>/N$.

Furthermore, because the structural robustness measure f_c is the critical fraction of attacks at which the network completely collapses, it ignores situations in which the network suffers a big damage without completely collapsing. To demonstrate the impact of attack information in depth, we also consider the network robustness measure R defined as[21, 22]

$$R = \frac{1}{N+1}\sum_{Q=0}^{N} S(Q) \tag{19}$$

where $S(Q)$ is the fraction of nodes in the largest component after removing $Q = Nf$ nodes in decreasing order of the displayed node degree $\tilde{d}$. The normalization factor $1/(N+1)$ ensures that the network robustness with different sizes can be compared. The network robustness R, which corresponds to the integral of the curves $S(Q)$, not only measures after how many removals the network collapse, but also considers the size of the largest component for each number of removed nodes. The range of possible R values is between $1/(N+1)$ and 0.5, where $R = 0$ corresponds to an empty network of isolated nodes and $R = 0.5$ corresponds a fully connected network.

The displayed degree distribution with imperfect attack information. For the purpose of convenience, let's suppose that the attack information perfection parameter α_i for all nodes is identical, i.e., $\alpha_i = \alpha$, $i = 1$, 2, …, N. Considering that the displayed degree $\tilde{d}_i$ follows a uniform distribution $U(a, b)$, we first formalize $\tilde{d}_i$ as

$$\begin{aligned}\tilde{d}_i &= a + (b-a)u \\ &= d_i\alpha + m(1-\alpha) + (M-m)(1-\alpha)u,\end{aligned} \tag{20}$$

where u is a random variable which follows a uniform distribution over the unit interval [0, 1]. Let $\Psi = d_i\alpha$ and $\Delta = m(1-\alpha) + (M-m)(1-\alpha)u$, then we obtain that

$$\tilde{d}_i = \Psi + \Delta. \tag{21}$$

Noting that

$$p_d(k) = \begin{cases} ck^{-\lambda} & m \le k \le M \\ 0 & \text{others} \end{cases}, \tag{22}$$

where $c \approx (\lambda - 1)m^{\lambda-1}$ and $M \approx mN^{1/(\lambda-1)}$[30]. We then obtain

$$p_\Psi(k) = \begin{cases} c'k^{-\lambda} & m\alpha \le k \le M\alpha \\ 0 & \text{others} \end{cases}, \tag{23}$$

where $c' = \alpha^{\lambda-1}(\lambda-1)m^{\lambda-1}$. Moreover, it is easy to obtain

$$p_{\Delta}(k) = \begin{cases} 1/(M-m)(1-\alpha) & m(1-\alpha) \le k \le M(1-\alpha) \\ 0 & \text{others} \end{cases}. \tag{24}$$

Consequently, we can obtain the probability distribution of displayed degree $\tilde{d}$ using the convolution formula

$$p_{\tilde{d}}(k) = \int_{t=-\infty}^{t=+\infty} p_{\Psi}(t)p_{\Delta}(k-t)dt = \int_{t=m\alpha}^{t=M\alpha} p_{\Psi}(t)p_{\Delta}(k-t)dt. \tag{25}$$

The critical removal fraction with imperfect attack information. In this study, we use the generating function formalism[31, 32] to derive the critical removal fraction f_c in random scale-free networks. We first sort all nodes in decreasing order of $\tilde{d}$. Denote by $r(\tilde{k})$ the rank of a node with the displayed degree $\tilde{k}$. Denote by $\tilde{K}$ the maximum displayed degree among the remaining nodes after a fraction f of nodes are removed in decreasing order of $\tilde{d}$. Noting that

$$r(\tilde{K}) = N \sum_{k=\tilde{K}+1}^{M} p_{\tilde{d}}(k) = Nf. \tag{26}$$

Then $\tilde{K}$ can be obtained by solving Eq. (26).

Denote by $q(k)$ the probability that a node with degree k is not removed. It equals to the probability that the displayed degree $\tilde{d}$ of a node with degree k is not larger than than $\tilde{K}$. Considering that $\tilde{d}$ is stochastic and follows the uniform distribution in the region $[k\alpha + m(1-\alpha), k\alpha + M(1-\alpha)]$. Then we can formalize $q(k)$ as

$$q(k) = \begin{cases} 0 & \tilde{K} < k\alpha + m(1-\alpha) \\ \dfrac{\tilde{K} - k\alpha - m(1-\alpha)}{(M-m)(1-\alpha)} & k\alpha + m(1-\alpha) \le \tilde{K} \le k\alpha + M(1-\alpha) \\ 1 & \tilde{K} > k\alpha + M(1-\alpha) \end{cases} \tag{27}$$

Noting that a giant component forms under the critical condition[28]

$$\frac{\sum_k k(k-1)p(k)q(k)}{\sum_k kp(k)} = 1. \tag{28}$$

Substituting Eq. (27) into Eq. (28), we can solve the critical removal fraction f_c.

References

1. Watts, D. J. & Strogatz, S. H. Collective dynamics of 'small-world' networks. *Nature* **393**, 440–442 (1998).
2. Barabási, A. L. & Albert, R. Emergence of scaling in random networks. *Science* **286**, 509–512 (1999).
3. Alderson, D. L. Catching the 'network science' bug: Insight and opportunity for the operations researcher. *Oper. Res.* **56**, 1047–1065 (2008).
4. Albert, R. & Barabási, A. L. Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74**, 47–51 (2002).
5. Newman, M. E. J. The structure and function of complex networks. *SIAM Rev.* **45**, 167–256 (2003).
6. Amaral, L. A. N. & Ottino, J. M. Complex networks - augmenting the framework for the study of complex systems. *Eur. Phys. J. B* **38**, 147–162 (2004).
7. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D. U. Complex networks: Structure and dynamics. *Phys. Rep.* **424**, 175–308 (2006).
8. Amaral, L. A. N. & Uzzi, B. Complex systems - a new paradigm for the integrative study of management, physical, and technological systems. *Manag. Sci.* **53**, 1033–1035 (2007).
9. Hellmann, T. & Staudigl, M. Evolution of social networks. *Eur. J. Oper. Res.* **234**, 583–596 (2014).
10. Wu, J., Deng, H.-Z., Tan, Y.-J. & Zhu, D.-Z. Vulnerability of complex networks under intentional attack with incomplete information. *J. Phys. A* **40**, 2665–2671 (2007).
11. Wu, J., Barahona, M., Tan, Y.-J. & Deng, H.-Z. Spectral measure of robustness in complex networks. *IEEE Trans. Syst., Man, Cybern. A* **41**, 1244–1252 (2011).
12. Dekker, A. H. & Colbert, B. Scale-free networks and robustness of critical infrastructure networks. In *7th Asia-Pacific Conference on Complex Systems*, 685–699 (2004).
13. Dekker, A. H. Simulating network robustness for critical infrastructure networks. In *28th Australasian conference on Computer Science*, 59–68 (Australian Computer Society, 2005).
14. Alderson, D. L., Brown, G. G., Carlyle, W. M. & Wood, R. K. Solving defender-attacker-defender models for infrastructure defense. In Dell, R. W. & R. F. (eds) *12th INFORMS Computing Society Conference*, 28–49 (INFORMS, 2011).
15. Estrada, E. Food webs robustness to biodiversity loss: The roles of connectance, expansibility and degree distribution. *J. Theor. Biol.* **244**, 296–307 (2007).
16. Sahasrabudhe, S. & Motter, A. E. Rescuing ecosystems from extinction cascades through compensatory perturbations. *Nature Commu.* **2**, 170 (2010).
17. Albert, R., Jeong, H. & Barabási, A. L. Error and attack tolerance of complex networks. *Nature* **406**, 378–382 (2000).
18. Carlson, J. M. & Doyle, J. Complexity and robustness. *Proc. Natl. Acad. Sci. USA* **99**, 2538–2545 (2002).
19. Doyle, J. C. *et al.* The "robust yet fragile" nature of the internet. *Proc. Natl. Acad. Sci. USA* **102**, 14497–14502 (2005).
20. Molloy, M. & Reed, B. A critical point for random graphs with a given degree sequence. *Random Struct. Algor.* **6**, 161–179 (1995).
21. Herrmann, H. J., Schneider, C. M., Moreira, A. A., Andrade, J. S. & Havlin, S. Onion-like network topology enhances robustness against malicious attacks. *J. Stat. Mech.* P01027 (2011).
22. Schneider, C. M., Moreira, A. A., Andrade, J. S., Havlin, S. & Herrmann, H. J. Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. USA* **108**, 3838–3841 (2011).

23. Yang, Z., Tang, K. & Yao, X. Large scale evolutionary optimization using cooperative coevolution. *Inform. Sci.* **178**, 2985–2999 (2008).
24. Kleijnen, J. P. Kriging metamodeling in simulation: A review. *Euro. J. Oper. Res.* **192**, 707–716 (2009).
25. Erdös, P. & Rényi, A. On random graphs. *Publ. Math.* **6**, 290–297 (1959).
26. Zhang, G.-D., Li, Z., Zhang, B. & Halang, W. A. Understanding the cascading failures in indian power grids with complex networks theory. *Physica A* **392**, 3273–3280 (2013).
27. Bollobás, B. *Random Graphs*. (Academic Press, New York, 1985).
28. Cohen, R., Erez, K., ben Avraham, D. & Havlin, S. Resilience of the internet to random breakdowns. *Phys. Rev. Lett.* **85**, 4626–4628 (2000).
29. Cohen, R., Erez, K., ben Avraham, D. & Havlin, S. Breakdown of the internet under intentional attack. *Phys. Rev. Lett.* **86**, 3682–3685 (2001).
30. Wu, J., Tan, Y., Deng, H., Zhu, D. & Chi, Y. Relationship between degree-rank distributions and degree distributions of complex networks. *Physica A* **383**, 745–752 (2007).
31. Callaway, D. S., Newman, M. E. J., Strogatz, S. H. & Watts, D. J. Network robustness and fragility: percolation on random graphs. *Phys. Rev. Lett.* **85**, 5468–5471 (2000).
32. Newman, M. E. J., Strogatz, S. H. & Watts, D. J. Random graphs with arbitrary degree distributions and their applications. *Phys. Rev. E* **64**, 026118 (2001).

Acknowledgements

J.W. acknowledges the National Natural Science Foundation of China under Grant No. 71371185 and the Program for New Century Excellent Talents in University under Grant No. NCET-12-0141. X.L. acknowledges the Natural Science Foundation of China under Grant Nos 71301165 and 71522014. We thank Qiang Luo, Juan Zhao, Dong-Li Duan, Ye Deng and Yu Xiao for useful discussions and comments.

Author Contributions

J.W. and Z.L. designed research; J.W., S.-Y.T, Z.L. and Y.-J.T performed research; J.W. and S.-Y.T conducted the experiments; J.W., S.-Y.T, Z.L. and Y.-J.T analyzed the results; J.W., S.-Y.T, Z.L., Y.-J.T and X.L. wrote the paper.

Additional Information

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.